UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/586,343	07/14/2006	Tomohiro Iwama	WPMCO133105	2697

83758 7590 09/29/2009

Christensen O'Connor Johnson Kindness PLLC
1420 Fifth Avenue
Suite 2800
Seattle, WA 98101-2347

EXAMINER	
ADDY, ANTHONY S	

ART UNIT	PAPER NUMBER
2617	

MAIL DATE	DELIVERY MODE
09/29/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/586,343	IWAMA ET AL.	
	Examiner	Art Unit	
	ANTHONY S. ADDY	2617	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *14 July 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *2-5* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *2-5* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *14 July 2006* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☒ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *07/14/2006*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in response to applicant's preliminary amendment filed on July 14, 2006. **Claims 1** and **6-14** are cancelled. **Claims 2-5** are now pending in the present application.

Information Disclosure Statement

2. The references listed in the Information Disclosure Statement filed on July 14, 2006 have been considered by the examiner (see attached PTO-1449 form or PTO/SB/08A and 08B forms).

Priority

3. Should applicant desire to obtain the benefit of foreign priority under 35 U.S.C. 119(a)-(d) prior to declaration of an interference, a certified English translation of the foreign application must be submitted in reply to this action. 37 CFR 41.154(b) and 41.202(e).

Failure to provide a certified translation may result in no benefit being accorded for the non-English application.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. **Claim 2** is rejected under 35 U.S.C. 102(e) as being anticipated by **Henry et al., U.S. Patent Number 7,441,043 (hereinafter Henry)**.

Regarding **claim 2,** Henry teaches a mobile wireless terminal apparatus (*e.g., a mobile network access device 200*) in a mobile wireless communication system which has a public network (*e.g., the Internet*), a private network (*e.g., corporate Intranet 218*) and a public wireless LAN system (*e.g., public WLAN 220*) and comprises a virtual private network relay apparatus which establishes an IPsec tunnel (*i.e., the virtual private network relay apparatus reads on the secure mobility gateway for establishing a mobile IPsec tunnel when the mobile device 200 is connected to the corporate intranet via the Internet*) with a network relay apparatus installed on the private network (*e.g., a gateway identified as GW on the Intranet 218*) via the public network (*i.e., the Internet*), further establishes the IPsec tunnel with the mobile wireless terminal apparatus (*i.e., the network access device 200*) and relays connection of the mobile wireless terminal apparatus (*200*) from the public wireless LAN system (*220*) to the private network (*218*) (see col. 5, lines 29-47, col. 18, lines 40-67 and fig. 2), a home agent that controls moving of the mobile wireless terminal apparatus (see col. 12, lines 17-20), a connection authentication server (*e.g., a centralized authentication server such as a Radius server or AAA*) that is installed on the public wireless LAN system and authenticates connection of the mobile wireless terminal apparatus to the public wireless LAN system, and a wireless LAN access point (*e.g., an AP within public WLAN*) that relays connection authentication procedures of a public wireless LAN performed between the mobile wireless terminal apparatus and the connection authentication server (see col. 7, lines 40-65 and fig. 2), comprising:

an authentication processing section that performs authentication processing of connection to the public wireless LAN system to the connection authentication server (*i.e., the authenticating processing section reads on an IRC client installed on the mobile host 200, since the IRC client is responsible for authenticating the user or the user's computer and creating a secure wireless connection to authenticate the user to a corporate network*) (see col. 5, lines 32-47, col. 10, lines 60-67 and col. 14, lines 44-63);

an address acquiring section that acquires an IP address of the virtual private network relay apparatus (*e.g., an IP address of the SMG's public interface IP_{SMG} reads on an IP address of the virtual private network relay apparatus*) from the connection authentication server when the connection to the public wireless LAN system is permitted (see col. 10, lines 60-67 and col. 17, lines 1-13); and

an address notifying section that notifies an IP address of the mobile wireless terminal (*e.g., an IP address of the user's computer IP_{MH} reads on an IP address of the mobile wireless terminal*) apparatus to the connection authentication server (see col. 10, lines 60-67 and col. 17, lines 1-10);

an IPsec key exchanging section that performs an IPsec key exchange with the virtual private network relay apparatus (*i.e., SMG*) using the IP address of the virtual private network relay apparatus (*i.e., reads on the teaching that the IRC client establishes an IPsec tunnel (IRC-SMG tunnel) between the user computer and the IPsec gateway using IKE (Internet Key Exchange) protocol, wherein the SMG is a special mobile IPsec gateway*) (see col. 9, lines 54-56, col. 11, lines 14-38 and col. 12, lines 3-5, col. 18, lines 40-49).

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

7. **Claims 3-5** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Henry et al., U.S. Patent Number 7,441,043 (hereinafter Henry)** and further in view of **Oyama et al., U.S. Publication Number 2006/0185013 A1 (hereinafter Oyama)**.

Regarding **claim 3,** Henry teaches a mobile wireless terminal apparatus (*e.g., a mobile network access device 200*) in a mobile wireless communication system which has a public network (*e.g., the Internet*), a private network (*e.g., corporate Intranet 218*) and a public wireless LAN system (*e.g., public WLAN 220*) and comprises a virtual private network relay apparatus which establishes an IPsec tunnel (*i.e., the virtual private network relay apparatus reads on the secure mobility gateway for establishing a mobile IPsec tunnel when the mobile device 200 is connected to the corporate intranet via the Internet*) with a network relay apparatus installed on the private network (*e.g., a gateway identified as GW on the Intranet 218*) via the public network

(*i.e., the Internet*), further establishes the IPsec tunnel with the mobile wireless terminal apparatus (*i.e., the network access device 200*) and relays connection of the mobile wireless terminal apparatus (*200*) from the public wireless LAN system (*220*) to the private network (*218*) (see col. 5, lines 29-47, col. 18, lines 40-67 and fig. 2), a home agent that controls moving of the mobile wireless terminal apparatus (see col. 12, lines 17-20), a connection authentication server (*e.g., a centralized authentication server such as a Radius server or AAA*) that is installed on the public wireless LAN system and authenticates connection of the mobile wireless terminal apparatus to the public wireless LAN system, and a wireless LAN access point (*e.g., an AP within public WLAN*) that relays connection authentication procedures of a public wireless LAN performed between the mobile wireless terminal apparatus and the connection authentication server (see col. 7, lines 40-65 and fig. 2), comprising:

an authentication processing section that performs authentication processing of connection to the public wireless LAN system to the connection authentication server (*i.e., the authenticating processing section reads on an IRC client installed on the mobile host 200, since the IRC client is responsible for authenticating the user or the user's computer and creating a secure wireless connection to authenticate the user to a corporate network*) (see col. 5, lines 32-47, col. 10, lines 60-67 and col. 14, lines 44-63).

Henry fails to explicitly teach an IPsec shared key acquiring section that acquires an IPsec pre-shared secret key for use in the IPsec key exchange performed with the virtual private network relay apparatus from the connection authentication server when the connection to the public wireless LAN system is permitted; and an IPsec key exchanging section that performs the

IPsec key exchange with the virtual private network relay apparatus using the IPsec pre-shared secret key.

In an analogous field of endeavor, Oyama teaches utilizing an Authorizing, Authentication, Accounting (AAA) server to transfer HMIPv6-related information required for authenticating and authorization a mobile node for HMIPv6 service over the AAA infrastructure (see abstract). For example, Oyama teaches a mobile node (MN) acquires an IPsec shared key for use in an IPsec key exchange performed with a Mobility Anchor Point (MAP) (*i.e., reads on a virtual private network relay apparatus*) from an AAA server (see p. 8 [0115, 0117 & 0119]). Oyama, further teaches the mobile node (MN) acquires a pre-shared secret key for use in mobile IP registration (*i.e., requesting to be authenticated and given MIPv6 service*) made with a home agent (HA) from an AAA server (see p. 8 [0130, 0132 & 0134]).

It would therefore have been obvious to one of ordinary skill in the art at the time of the invention to modify Henry with the teachings of Oyama to include a mobile wireless terminal apparatus acquiring an IPsec pre-shared secret key for mobile IP registration, in order to efficiently transfer information for authenticating and authorizing a mobile node requesting mobile IP related services over an AAA infrastructure to secure pertinent communication as taught by Oyama (see p. 3 [0033, 0035, 0038 & 0060]).

Regarding **claim 4,** Henry teaches a mobile wireless terminal apparatus (*e.g., a mobile network access device 200*) in a mobile wireless communication system which has a public network (*e.g., the Internet*), a private network (*e.g., corporate Intranet 218*) and a public wireless LAN system (*e.g., public WLAN 220*) and comprises a virtual private network relay apparatus which establishes an IPsec tunnel (*i.e., the virtual private network relay apparatus reads on the*

secure mobility gateway for establishing a mobile IPsec tunnel when the mobile device 200 is connected to the corporate intranet via the Internet) with a network relay apparatus installed on the private network (*e.g., a gateway identified as GW on the Intranet 218*) via the public network (*i.e., the Internet*), further establishes the IPsec tunnel with the mobile wireless terminal apparatus (*i.e., the network access device 200*) and relays connection of the mobile wireless terminal apparatus (*200*) from the public wireless LAN system (*220*) to the private network (*218*) (see col. 5, lines 29-47, col. 18, lines 40-67 and fig. 2), a home agent that controls moving of the mobile wireless terminal apparatus (see col. 12, lines 17-20), a connection authentication server (*e.g., a centralized authentication server such as a Radius server or AAA*) that is installed on the public wireless LAN system and authenticates connection of the mobile wireless terminal apparatus to the public wireless LAN system, and a wireless LAN access point (*e.g., an AP within public WLAN*) that relays connection authentication procedures of a public wireless LAN performed between the mobile wireless terminal apparatus and the connection authentication server (see col. 7, lines 40-65 and fig. 2), comprising:

an authentication processing section that performs authentication processing of connection to the public wireless LAN system to the connection authentication server (*i.e., the authenticating processing section reads on an IRC client installed on the mobile host 200, since the IRC client is responsible for authenticating the user or the user's computer and creating a secure wireless connection to authenticate the user to a corporate network*) (see col. 5, lines 32-47, col. 10, lines 60-67 and col. 14, lines 44-63).

Henry fails to explicitly teach an MIP shared key acquiring section that acquires a pre-shared secret key for use in mobile IP registration made with the home agent from the connection

authentication server when the connection to the public wireless LAN system is permitted; and an MIP registering section that makes the mobile IP registration to the home agent using the pre-shared secret key.

In an analogous field of endeavor, Oyama teaches utilizing an Authorizing, Authentication, Accounting (AAA) server to transfer HMIPv6-related information required for authenticating and authorization a mobile node for HMIPv6 service over the AAA infrastructure (see abstract). For example, Oyama teaches the mobile node (MN) acquires a pre-shared secret key for use in mobile IP registration (*i.e., requesting to be authenticated and given MIPv6 service*) made with a home agent (HA) from an AAA server (see p. 8 [0130, 0132 & 0134]).

It would therefore have been obvious to one of ordinary skill in the art at the time of the invention to modify Henry with the teachings of Oyama to include a mobile wireless terminal apparatus acquiring an IPsec pre-shared secret key for mobile IP registration, in order to efficiently transfer information for authenticating and authorizing a mobile node requesting mobile IP related services over an AAA infrastructure to secure pertinent communication as taught by Oyama (see p. 3 [0033, 0035, 0038 & 0060]).

Regarding **claim 5,** Henry teaches a mobile wireless terminal apparatus (*e.g., a mobile network access device 200*) in a mobile wireless communication system which has a public network (*e.g., the Internet*), a private network (*e.g., corporate Intranet 218*) and a public wireless LAN system (*e.g., public WLAN 220*) and comprises a virtual private network relay apparatus which establishes an IPsec tunnel (*i.e., the virtual private network relay apparatus reads on the secure mobility gateway for establishing a mobile IPsec tunnel when the mobile device 200 is connected to the corporate intranet via the Internet*) with a network relay apparatus installed on

the private network (*e.g., a gateway identified as GW on the Intranet 218*) via the public network (*i.e., the Internet*), further establishes the IPsec tunnel with the mobile wireless terminal apparatus (*i.e., the network access device 200*) and relays connection of the mobile wireless terminal apparatus (*200*) from the public wireless LAN system (*220*) to the private network (*218*) (see col. 5, lines 29-47, col. 18, lines 40-67 and fig. 2), a home agent that controls moving of the mobile wireless terminal apparatus (see col. 12, lines 17-20), a connection authentication server (*e.g., a centralized authentication server such as a Radius server or AAA*) that is installed on the public wireless LAN system and authenticates connection of the mobile wireless terminal apparatus to the public wireless LAN system, and a wireless LAN access point (*e.g., an AP within public WLAN*) that relays connection authentication procedures of a public wireless LAN performed between the mobile wireless terminal apparatus and the connection authentication server (see col. 7, lines 40-65 and fig. 2), comprising:

an authentication processing section that performs authentication processing of connection to the public wireless LAN system to the connection authentication server (*i.e., the authenticating processing section reads on an IRC client installed on the mobile host 200, since the IRC client is responsible for authenticating the user or the user's computer and creating a secure wireless connection to authenticate the user to a corporate network*) (see col. 5, lines 32-47, col. 10, lines 60-67 and col. 14, lines 44-63);

an address acquiring section that acquires an IP address of the virtual private network relay apparatus (*e.g., an IP address of the SMG's public interface IP_{SMG} reads on an IP address of the virtual private network relay apparatus*) from the connection authentication server when

the connection to the public wireless LAN system is permitted (see col. 10, lines 60-67 and col. 17, lines 1-13); and

an address notifying section that notifies an IP address of the mobile wireless terminal (*e.g., an IP address of the user's computer IP_{MH} reads on an IP address of the mobile wireless terminal*) apparatus to the connection authentication server (see col. 10, lines 60-67 and col. 17, lines 1-10);

Henry fails to explicitly teach an IPsec shared key acquiring section that acquires an IPsec pre-shared secret key for use in the IPsec key exchange performed with the virtual private network relay apparatus from the connection authentication server; an MIP shared key acquiring section that acquires an MIP pre-shared secret key for use in mobile IP registration made with the home agent from the connection authentication server; an IPsec key exchanging section that performs exchange of the IPsec key with the virtual private network relay apparatus using the IPsec pre-shared secret key; and an MIP registering section that makes the mobile IP registration to the home agent using the MIP pre-shared secret key.

In an analogous field of endeavor, Oyama teaches utilizing an Authorizing, Authentication, Accounting (AAA) server to transfer HMIPv6-related information required for authenticating and authorization a mobile node for HMIPv6 service over the AAA infrastructure (see abstract). For example, Oyama teaches a mobile node (MN) acquires an IPsec shared key for use in an IPsec key exchange performed with a Mobility Anchor Point (MAP) (*i.e., reads on a virtual private network relay apparatus*) from an AAA server (see p. 8 [0115, 0117 & 0119]). Oyama, further teaches the mobile node (MN) acquires a pre-shared secret key for use in mobile

IP registration (*i.e., requesting to be authenticated and given MIPv6 service*) made with a home agent (HA) from an AAA server (see p. 8 [0130, 0132 & 0134]).

It would therefore have been obvious to one of ordinary skill in the art at the time of the invention to modify Henry with the teachings of Oyama to include a mobile wireless terminal apparatus acquiring an IPsec pre-shared secret key for mobile IP registration to a home agent, in order to efficiently transfer information for authenticating and authorizing a mobile node requesting mobile IP related services over an AAA infrastructure to secure pertinent communication as taught by Oyama (see p. 3 [0033, 0035, 0038 & 0060]).

Conclusion

8. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Giaretta et al., U.S. Publication Number 2007/0230453 A1 discloses method and system for the secure and transparent provision of mobile IP services in an AAA environment.

Amara et al., U.S. Patent Number 6,839,338 discloses method to provide dynamic internet protocol security policy service.

Song et al., U.S. Patent Number 7,065,067 discloses authentication method between mobile node and home agent in a wireless communication system.

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to ANTHONY S. ADDY whose telephone number is (571)272-7795. The examiner can normally be reached on Mon-Thur 8:00am-6:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Patrick Edouard can be reached on 571-272-7603. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Anthony S Addy/
Examiner, Art Unit 2617